

Using Preferences as User Identification in the Online Examination

Nader Abdel Karim^{*1}, Zarina Shukur²

^{*}Research Center for Software Technology and Management, Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia, 43600, Bangi, Selangor, Malaysia.
E-mail: ¹nader_cisco@hotmail.com, ²zarinashukur@ukm.edu.my

Abstract— User authentication is a very important online environment issue. More researches are needed to focus on enhancing user authentication methods for online examination. This paper is a review of online authentication methods for online examination and propose a novel authentication method called “Preferences Based Authentication” PrBA. The proposed method based on the exam taker design preferences chosen for online exams. A lot of design features could be applied to the exam interface, such as font (size, face, and style, colour), background colour, the number of questions per page, group question by (Type, difficulty) and timer type. These preferences have a close relationship with user characteristics, whether physical (vision, hearing, etc.), cognitive (memory, etc.), psychomotor (attention, focus, etc.), demographics (age, gender, etc.) or experiences (professional skills). The PrBA proposed in this paper could be used as an alternative to resolve the problem of user authentication within online exams.

Keywords—user authentication; authentication methods; online exam; user preferences; interface design

I. INTRODUCTION

The development of the Internet has largely changed learning and teaching from a traditional classroom into an invaluable educational resource available distantly from dispersing geographical locations, outside physical limitations. E-learning can lead to a better future, as we advance in all areas of science that are needed in this modern life. based on the report of Global Industry Analyst, the global e-learning market is expected to touch \$107.3 billion by 2015 [1].

The E-learning environments are likely to be accessible, available, updatable, resource efficient, usable, economical [2] and have been usually accepted by a lot of universities, colleges and educational institutions in various disciplines [1]. In the E-learning, the examination is combined with the teaching and learning components. In an online examination scenario, there probably no face-to-face communication between teachers, students, and administrators [4], therefore, user authentication is vital to the authority of E-learning environments. Due to the nature of E-learning environments makes it more susceptible to a lot of security threats [5]. Online examinations being an essential part of the learning environment can be high stake applications, which could fall to impersonation and malicious attacks for higher marks [1], [6], [7]. User authentication is a widely discussed subject in online environments [8]. The main aim of user authentication is to ensure that the person how is interacting with online examination is a genuine user.

Essentially online exams follow identifications, such as username, password and biometric authentication [9]. In general, user authentication is divided into three main categories which are something you knows (knowledge-based authentication), something you has (Possession-based authentication), and something you are (biometric-based authentication) [10], [11].

This paper is presented as follows: Section II is an overview of online examination authentication methods and online exam user authentication threats; Section III discusses the proposed method and Section IV summarises the paper, and proposes future research directions.

II. MATERIALS AND METHODS

A. Online Exam Authentication Methods

Most computer systems are protected through a process of user authentication [12], [13]. Authentication provides secret and private information. In general authentication methods can be classified into In general, authentication methods can be classified as knowledge, possession or biometric based (see Fig. 1).

1) *Knowledge-Based Authentication (KBA)*: The most widely used types of authentication is knowledge-based [12]. KBA requires the knowledge of private information of an individual to grant access to protected material. User ID, password and challenge questions are commonly used. KBA is a common authentication method because passwords are memorable, cheap, easy to use, and attractive to users [5],

[12]. However, due to the nature of online exams, users may pass their login information to third parties to increase their grades. Hence, online examinations rely on a knowledge base that is susceptible to collusion and impersonation threats [5].

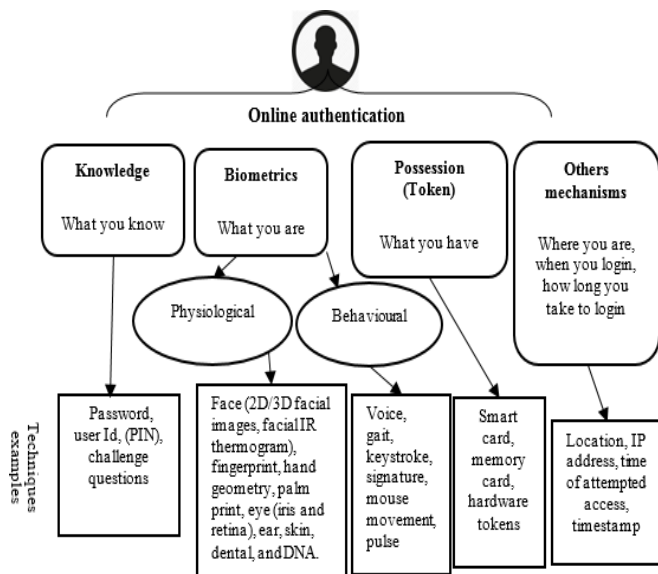


Fig. 1 Online user-authentication methods

2) *Possession Based Authentication (PBA)*: PBA is the type of authentication based on private objects that the user has; sometimes it's called token-based authentication (token). PBA includes tokens and tickets. A token is typically a hardware device that can be stored and carried with the user. However, in general, showing of a valid token does not prove possession; because it may have been stolen or copied by others [12]. Based on the nature of online exams, PBA can be useful if the exam is conducted in a specific place, such as college labs or in qualified testing centres. However, if the exam is conducted at home or in any place outside campus with no physical control, PBA is useless. The popular examples of the PBA are; memory cards, smart card tokens, dongles, and keys [10], [12].

3) *Biometrics-Based Authentication (BBA)*: Biometrics is a new technology that is used to enhance security in the applications [6]. It is also defined as the identification of a user that depends on physiological and behavioural characteristics. Physiological biometrics refers to are based on the user's physical characteristics. Commonly used physiological characteristics include Face (2D/3D Facial images, facial IR thermograms), Hand (fingerprints, hand geometry, palm prints, hand IR thermograms), Eye (iris and retina), Ear, Skin, Dental, and DNA. Behavioural biometrics are based on the user's behavioural characteristics that are considered as learned movements [12]. Commonly used behavioural characteristics include; voice, gait, signature, mouse movement, keystroke and pulse [14], [12]. Biometric authentications are technically complex and usually expensive because they require special hardware [12]. The appearance of biometrics solved the problems that plagued traditional authentication methods [14], [12]. They provide the most effective and accurate identification methods because they cannot be

easily stolen or shared. Biometric systems can enhance user convenience by lessening the need to design and remember passwords [15]. However, biometrics authentication is not widely accepted by users; because they are perceived as intrusive and a violation of personal privacy. In biometric systems, biometric data has to be saved in a centralized database or distributed on smart cards. Potential biometrics users are reluctant to give out their biometric data because they are worried how their biometric data will be used, for what purpose, and whether their biometric data will be protected adequately [14], [12].

There are many other authentication mechanisms that can help in user authentication process, such as location, timestamp, IP address and time of attempted access. Table 1 gives a brief summary of existing authentication techniques that can be used in online examinations. The table shows the techniques and classifications, in addition to a brief description of each technique. Finally, several example references are given.

TABLE I
AUTHENTICATION TECHNIQUES USED IN ONLINE EXAMINATION

Technique	Technique classification	Description	References example
user_id	Knowledge Based authentication	Based on private information supplied by the user.	[5], [16], [17]
Password			
Challenge questions			
Mouse movement	Behavioural biometric	Behavioural characteristics. Can be used in continuous authentication.	[18], [19]
Keystroke dynamics			[19], [20], [21]
Voice		Behavioural characteristics. Voice verification using a microphone. Can be used as continuous authentication.	[22]
Signature		Behavioural characteristics.	[17]
Stylometry		Behavioural characteristics. Determines authorship from the linguistic styles of the authors.	[20], [23]
Handwriting		There are two types of handwriting-based authentication: one based on static information (letter width, density) and one based on dynamic information (x and y coordinates, writing speed, writing pressure and pen angle). Can be	[24]

		applied to online exams using pen tablets or touch screens.	
Face recognition	Physiological Biometrics	Can be used in continuous authentication.	[25], [6], [19], [26], [27]
Fingerprint		Can be used in continuous user authentication; if it is included with other devices, such as a fingerprint-scanning mouse.	[6], [25] [14], [28]
Eye tracking		The eye feature tracking for validating users.	[29]
Brainwaves		ERP (Event Related Potential). Signals used to explain the cognitive information process. Can be used to show differences between e-learning users.	[29]
Palm-print		Physiological characteristics. Needs additional devices to scan (palm print scanning device).	[16]
Smart card, memory card & zip disk	Possession based authentication	Based on private objects that the user possesses. Maybe stolen or duplicated by sophisticated means.	[30]
IP address	Other-mechanisms*	Can be used to identify the possible location of a user. IP address (together with a timestamp) can be used as indicators of possible cheating behaviour during exams.	[9], [28]
Timestamp		Used to know at which time the exam session started.	[30]
Webcam		Can be used in continuous presence authentication.	[31], [32]
Video monitoring		Can be used in continuous presence authentication.	[16], [30], [9]
* Other-mechanisms equate to other authentication methods that may help in user authentication that is not classified as knowledge, possess or biometric based authentications, such as user location, IP address, time of attempted access and timestamp, in addition to user presence authentication techniques, such as webcam and video monitoring.			

B. Online Exam User Authentication Threats

Based on the code of practice for the Assurance of Academic Quality and Standards in Higher Education (QAA) in the UK, the meanings of academic misconduct, in respect of assessment, include plagiarism, collusion, impersonation and the use of inadmissible material [33]. In general, one of the main security challenges to user security in online environments; especially in online exams, is the action of impersonation. Impersonation is considered to be a fake action with the goal of duplicating an authentic user and defrauding the security system. In an online exam, the issue of impersonation is considered the most important cause of concern and is therefore considered to be a greater risk by the academic community [6], [34]. Based on the literature in [18], [35], there is a significant possibility of impersonation threats during online exams. Impersonation can be direct by allowing Another person attempts to take the exam on behalf of the true user ,or indirect impersonation; where the original user sits to take the exam, but the assistant answers the questions [13].

C. Commercial Systems for Proctoring Online-Exam

Nowadays, there are current commercial systems that deal with user authentication issue in online examination . Based on the literatures, there are at least 5 systems that have been received by several universities and colleges, for their online courses, namely ProctorU, ProctorCam, Webassessor BioSig-ID and Secureexam. Payment is required for protecting each online exam session or on each individual in case of use this kind of systems.

In the main, these authentication systems try to stop the cheating in the online-exam by merging both conventional knowledge-based authentication (user_name,password) with biometrics-based authentication (such as Fingerprint). Table 2 summarize each of these systems.

TABLE II
COMMERCIAL ONLINE-EXAMINATION REMOTE PROCTOR SYSTEMS

Systems Name	Description	Example University
Secureexam Remote Proctor (SRP) http://www.remoteproctor.com	The fingerprint for student identification.	Troy University, New York University
ProctorU , Axicom Corp http://www.proctoru.com (Virtual online proctoring)	Username, password, and ID photo for student identification. Human proctor in real-time and video surveillance system /audio recording	National American University, Andrew Jackson University
ProctorCam http://www.proctorcam.com (Virtual online proctoring)	Username, password, and ID photo for student identification. Human proctor in real-time and video surveillance system /audio recording	Boston University's Metropolitan College, Loyola University C hicago's

WebassessorTM (http://www.kryteri.ononline.com/)	Facial recognition software and patterns of keystroke rhythms. Secure Browser Control video surveillance system	Penn State University
BioSig-ID	The login into system needs a username, first name and last name. after that users must select the pointing device that will be used to draw their signature (e.g. a mouse, a stylus, or touch pad)	The university of Texas Systems ,University of Maryland, and Houston Community College

D. Preference Based Authentication-PrBA

Recent developments in the technology and the use of the Internet worldwide emerges the importance of user interfaces [36],[37]. New technologies are developing for user comfort. Therefore, user interfaces are becoming the main discriminator for the products [38]. McDaniel ,1994 defines user interface as follows [39]:

“Hardware, software (including menus, screen design, keyboard commands, and command language), or both that allow a user to interact with and perform operations on a system, program, or device” (p. 724)

The user interface is very important part of any software application, one that often determines how well software users learn ,accept, and efficiently work with entire systems [40] Whatever the underlying technology is, users can contact the system through the user interface [41], [42]. Furthermore, the Internet provides information to people all around the world. These people from different cultures have different characteristics such as perceptions, cognition, thinking styles, and values etc. [43].

The online exam is a very important system within E-Learning environment. Students dealing with online exam periodically during the study period. User characteristics have a direct impact on how interface design will be [44], [43]. Therefore, the online exam interface design must take user characteristics into consideration. Refereeing to literature [44], [45] the classification of user characteristics that can impact on the user interface design and examples on each one are shown in Fig. 2 which shows that the user characteristics has been classified into Physical, Psychomotor, Cognitive, Psychological, Demographics, and Experience.

Nowadays, many human computer interaction (HCI) researches are focusing on how to establish adaptive user interfaces to improve the usability of the systems and to enhance the user’s convenience in order to establish a suitable user interface based on the characteristics of the users [46],[47],[48](see Fig. 3).

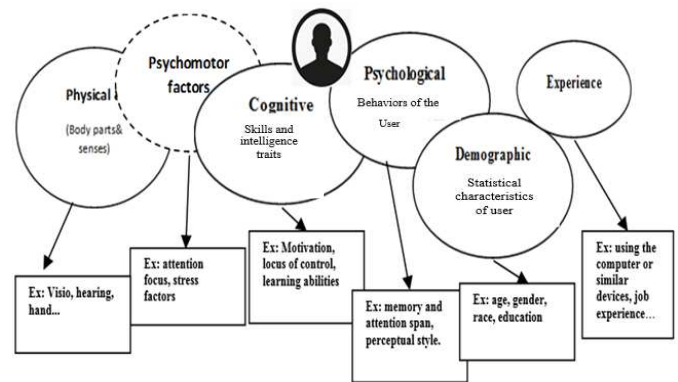


Fig. 2 User characteristics that could affect the interface design [37]

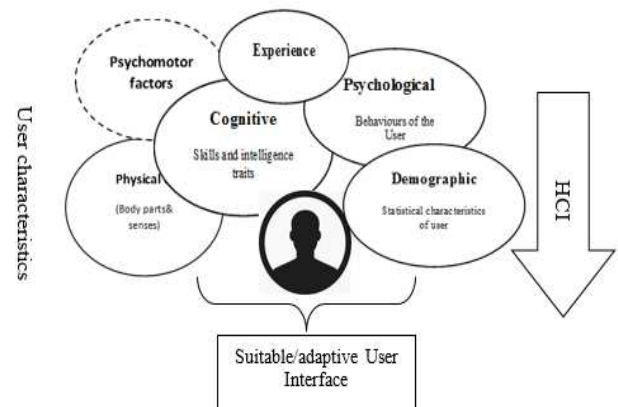


Fig. 3 Relationship between user characteristics and interface design

This was done in reverse in the proposed method by trying to identify the users based on their desired preferences. The authentication system would give users the opportunity to choose their own suitable interface design based on their characteristics.

Interface preferences are the alternative uses of interface elements, which form the entire user interface. Is there a relationship between user characteristics and user preferences? For instance Özgen,2008 [49] investigated the relationship between user characteristics and user’s interface preferences, 2500 participants from 120 different countries participate in his survey.

The results show that there is a relationship between users’ characteristics and users’ interface preferences. Moreover, Michael and Mills said there is a relationship between user characteristics and user font type [50]. Evers et. al [51] indicated that the design preferences do affect interface acceptance. Therefore, we can say that users’ characteristics will effect on interface preferences, and each individual has its own characteristics for that different interface design will appear. So that, the interface preferences would be used as evidence of the user’s identity in the same way that Ullah et al. used the challenge questions [5]. This method, which is called the PrBA method, takes note of the fact that challenge questions are not efficient enough [52], and that this extra step in the online exam may annoy users. On the other hand, the online exam interface preferences will be useful for students and allow them to pick their own suitable design, depending on their characteristics. This step aims to add convenience and takes into account individual differences among users in addition

to using it as a user authentication method to identify a user based on his or her selected preferences.

III. RESULTS AND DISCUSSION

Our proposed online-exam authentication system will consist of three phases: login phase, online-exam interface preferences phase, and exam session phase (refer Fig. 4).

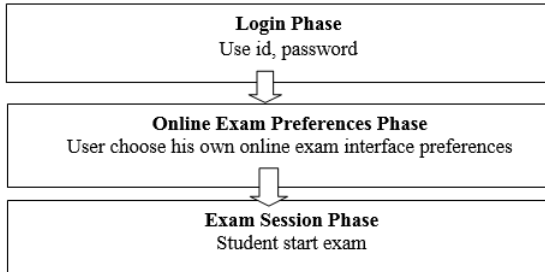


Fig. 4 Online exam authentication system phases

- *Login Phase:* User can enter the user_id and password to gain access if the user passes the login phase the system will redirect him to the online exam preferences page.
- *Online Exam Preferences Phase:* Online exam preferences page would give the user ability to choose his own preferred exam design depending on his characteristics, many online exam design features will be offered on this page (see Fig. 5). Such as font (face, size, style, colour), background colour, time counter (digital to down/ascending, traditional clock), sound alert, No. of questions/page and group questions by (Topic, difficulty, type) [37].
- *Exam Session Phase:* In this phase, the exam session would start, biometric based authentication could be used in this phase for continuous user authentication along exam period [25].

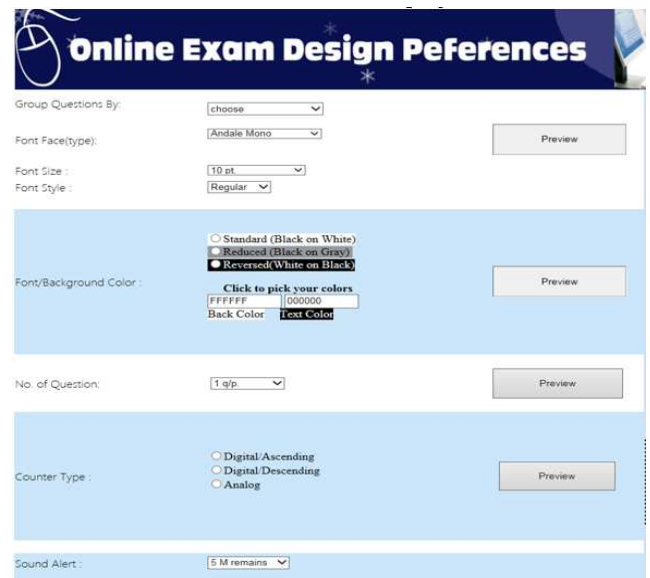


Fig. 5 Online exam design preferences web page

Fig. 6 shows the process model of proposed online-exam authentication system, the proposed system consist of two authentication phases, login authentication and preferences authentication. The following stages explain how the authentication system works starting from collecting student's data and ending with user verification process.

Stage 1: In this stage, two activities will be conducted before the real online exam session starts.

- *Registration:* As depicted in Fig. 6 the process starts from finishing registration to get login information. The students would create their own accounts and finished online registration. The registration process includes a selection of user-id, password, email address, birth date, gender, and educational level.

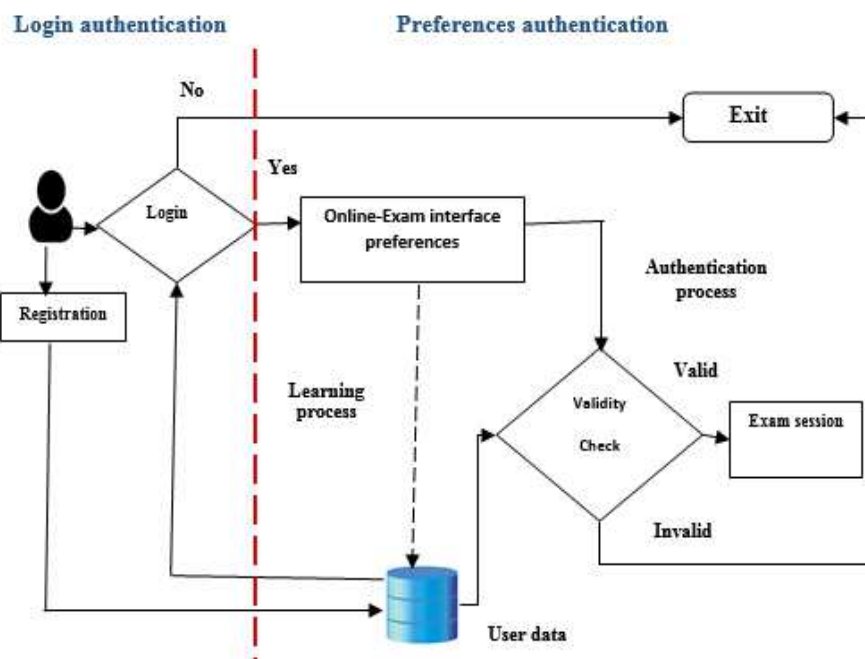


Fig. 6 Preferences Based Authentication (PrBA) process model

- *Learning Process:* After the registration, the student would be redirected to an exam preferences web page to choose his own “exam interface preferences” for the purpose of practice and training.

After the student finishes the practice the system confirms him to save the interface preferences which he had chosen, more than one preference templates would be saved for each student in different practice sessions. Then the data would be stored in the (user_id) Database in order to use it for comparison within a real online exam session.

Stage 2: In this stage, two activities will be conducted; login authentication and preferences authentication.

- *Login Authentication:* The student has 3 trails to login into online examination using his user_id and password if the user success he would be redirected to the “online-exam design preferences” web page, other than that the user would not be able to login to the system.
- *Interface Design Preferences Authentication:* In the authentication process, if the user’s “interface preference” matched the stored student preferences templates, the student would be granted access to online examination. If the design preferences do not match to the stored user templates, the student access would be blocked and the event is reported to the system administrator.

IV. CONCLUSIONS

User authentication methods can be knowledge, possession or biometric-based authentication. Each authentication method offers both advantages and disadvantages. Biometric based authentication is considered the most accurate and popular method authentication method used in the online exams. There are many user authentication threats that could affect on the online exam such as collusion, and impersonation. Impersonation impacts on the online exam credibility, it is considered the main threat in online exam environments. In this article, we propose an Online-Exam Authentication System. The system consists of two layers of authentication. The first layer is login authentication which based on the user_id and password. Whereas, the second one is PrBA which is based on the online exam interface design chosen by the user. PrBA depends on a certain principle which emphasizes that users' characteristics effect on the interface design and each individual has its own characteristics. Therefore, the online exam interface design that the exam-taker picked before an exam session started would give an evidence on the user identity. For future research, the experiment would be conducted in order to investigate the feasibility and accuracy of PrBA.

ACKNOWLEDGMENT

The authors would like to thank the faculty of information Science and Technology, Universiti Kebangsaan Malaysia by giving the authors an opportunity to conduct this research.

This work was supported by Universiti Kebangsaan Malaysia under research grant (DPP-2015-018).

REFERENCES

- [1] B. H. Xiao and W. Ji, “Authentication of Students and Students’ Work in E-Learning,” Report for the Development Bid of Academic Year 2010/11. University of Hertfordshire . July, pp. 1–49, 2011.
- [2] J. G. Ruiz, M. J. Mintzer, and R. M. Leipzig, “The impact of e-learning in medical education,” *Journal of Academic Medicine.*, vol. 81(3):207-212, 2006
- [3] S. Rodchua, “Student Verification System for Online Assessments: Bolstering Quality and Integrity of Distance Learning,” *Journal of Industrial Technology*, 27(3): 1- 8, 2011.
- [4] B. Hayes and J. Ringwood, “Authenticating student work in an e-learning programme via speaker recognition,” *Proceedings of the 3rd International Conference on Signals, Circuits and Systems (SCS)*, pp. 1–6, 2009.
- [5] A. Ullah, H. Xiao, M. Lilley, and T. Barker, “Using challenge questions for student authentication in online examination,” *International Journal of Infonomics*, vol. 5, no. 3, pp. 631–639, 2012.
- [6] K. Apampa, G. Wills, and D. Argles, “User security issues in summative e-assessment security”, *International Journal of Digital Society (IJDS)*, 1(2), pp. 135–147, 2010.
- [7] J. W. Gathuri and S. Kamundi, “Impersonation Challenges Associated With E-Assessment of University Students,” *Journal of Information Engineering and Applications*, vol. 4, no. 7, pp: 60-69, 2014.
- [8] B. Abdullateef, N. Elias, and H. Mohamed, “An evaluation and selection problems of OSS-LMS packages,” *SpringerPlus*, 5:248, 2016.
- [9] M. Sarayrih and M. Ilyas, “Challenges of Online Exam , Performances and problems for Online University Exam,” *International Journal of Computer Science Issues*, Vol. 10, Issue 1, pp. 439–443, January 2013.
- [10] N. Hastings and D. Dodson, “Quantifying assurance of knowledge based authentication”, *Proceedings of the 3rd European Conference on Information Warfare and Security*, pp 109-116, 2004.
- [11] B. Menkus, “Understanding the use of passwords,” *Journal of Computers and Security*, vol. 7, no. 2, pp. 132–136, 1988.
- [12] M. Zviran, “Identification and Authentication: Technology and Implementation Issues,” *Communications of the Association for Information Systems*, 17(1), pp. 90–105, 2006.
- [13] Z. Abdel Karim, Nader, Shukur, “Review of User Authentication Methods in Online Examination,” *Asian Journal of Information Technology*, 14(5), pp. 166–175, 2015.
- [14] Q. Gao, “Biometric Authentication to Prevent e-Cheating”, *International Journal of Instructional Technology & Distance Learning*, 9(2): 3-13, Feb. 2012.
- [15] B. Ives, K. R. Walsh, and H. Schneider, “The domino effect of password reuse,” *Communications of ACM Magazine*, vol. 47, no. 4, pp. 75–78, 2004.
- [16] [16] S. M. Al-Saleem and H. Ullah, “Security considerations and recommendations in computer-based testing,” *Scientific World Journal*, vol. 2014, Article ID. 562787, 2014.
- [17] V. Bhagat and V. Katankar, “Novel method for Student Authentication in Online Examination,” *International Journal of Research*, 1(7), pp. 974-979, 2014.
- [18] S. Asha and C. Chellappan, “Authentication of e-learners using multimodal biometric technology,” *Proceedings on the International Symposium on Biometrics and Security Technologies*, 2008. pp. 1–6, 2008.
- [19] M. K. Dehnavi and N. P. Fard, “Presenting a multimodal biometric model for tracking the students in virtual classes,” *Procedia Social and Behavioral Sciences*, vol. 15, pp: 3456–3462, 2011.
- [20] J. C. Stewart, “An Evaluation of the Application of Stylometry and the Keystroke Biometric to Identity Verification of Online Test-Takers,” PhD Thesis, Pace University, New York, USA, 2013.
- [21] A. Morales and J. Fierrez, “Keystroke Biometrics for Student Authentication: A Case Study,” *Proceedings of the ACM Conference on Innovation and Technology in Computer Science Education*, pp: 337-337, 2015.
- [22] D. Rudrapal, S. Das, S. Debbarma, N. Kar, and N. Debbarma, “Voice Recognition and Authentication as a Proficient Biometric Tool and Its Application in Online Exam for P.H People,” *International Journal of Computer Applications*, 39(12), pp: 6-12, February 2012.

- [23] M. Krause, "A behavioral biometrics based authentication method for MOOC's that is robust against imitation attempts," Proceedings of the first ACM Conference on Learning@scale, pp: 201-202, 2012.
- [24] S. Kikuchi, T. Furuta, and T. Akakura, "Periodical examinees identification in e-test systems using the localized arc pattern method," Proceedings of the Conference on Distance Learning and Internet, pp:213-220, 2018.
- [25] A. Moini and a. M. Madni, "Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective," IEEE Systems Journal, 3(4), pp. 469-476, 2009.
- [26] J. Valera, J. Valera, and Y. Gelogo, "A Review on Facial Recognition for Online Learning Authentication," Proceedings of the 8th International Conference on Bio-Science and Bio-Technology, pp: 16-19, 2015.
- [27] A. Prakash and R. Dhanalakshmi, "Stride Towards Proposing Multi-Modal Biometric Authentication for Online Exam," International Journal of Network Security, 18(4), pp: 678-687, July 2016.
- [28] P. Khanna, R. Sharma, and S. Shukla, "Developments, Performances and Challenges in Online Examination System," International Journal of Research in Computer Engineering and Electronics, 4(1), 2015.
- [29] K. Song, S. M. Lee, and S. Nam, "Combined biometrics for e-learning security," Proceedings of the 7th International Conference on Information Security and Assurance, vol. 21, pp. 247-251, 2013.
- [30] C. C. Ko and C. D. Cheng, "Flexible and secure computer-based assessment using a single zip disk," Computers and Education, vol. 50, no. 3, pp. 915-926, 2008.
- [31] K. Hylton, Y. Levy, and L. Dringus, "Utilizing webcam-based proctoring to deter misconduct in online exams," Computers and Education, vol. 92-92, pp:53-63, 2016.
- [32] A. Agrawal, A. Keshri, G. Athmika, and B. Jakkali, "Framework For Online Exam With Graphical Result and SMS Gateway," 3(2), pp: 31-33, 2016.
- [33] L. Bellingham, "Quality Assurance and the Use of Subject Level Reference Points in the UK," Quality in Higher Education, 14(3), pp: 265-276, 2008.
- [34] S. Kerka, M. E. Wonacott, C. Grossman, and J. Wagner, "Assessing Learners Online," Journal of Distance Learning, 23(1), pp:127-128, 2009.
- [35] N. C. Rowe, "Cheating in Online Student Assessment: Beyond Plagiarism," Online Journal of Distance Learning Administration, 7(2), pp: 1-10, 2004.
- [36] G. Calvary, J. Coutaz, D. Thevenin, Q. Limbourg, L. Bouillon, and J. Vanderdonckt, "A Unifying Reference Framework for multi-target user interfaces," Interacting with Computers, 15(3), pp. 289-308, 2003.
- [37] N. Karim and Z. Shukur, "Proposed features of an online examination interface design and its optimal values," Computers in Human Behaviour, vol.64, pp. 414-422, 2016.
- [38] K. S. Park and C. Hwan Lim, "A structured methodology for comparative evaluation of user interface designs using usability criteria and measures," International Journal of Industrial Ergonomics, 23(5-6), pp: 379-389, 1999.
- [39] G. McDaniel, "IBM Dictionary of Computing," p. 758, 1994.
- [40] A. R. Puerta, "Supporting User-Centered Design of Adaptive User Interfaces Via Interface Models," First Annual Workshop On Real-Time Intelligent User Interfaces For Decision Support And Information Visualization, San Francisco, 1998.
- [41] P. A. Chalmers, "The role of cognitive theory in human-computer interface," Computers in Human Behavior, 19(5), pp. 593-607, 2003.
- [42] A. Agah and K. Tanie, "Intelligent graphical user interface design utilizing multiple fuzzy agents," Interacting with Computers, 12(5), pp. 529-542, 2000.
- [43] P.L. P. Rau, Y.Y. Choong, and G. Salvendy, "A cross cultural study on knowledge representation and structure in human computer interfaces," International Journal of Industrial Ergonomics, vol. 34, no. 2, pp. 117-129, 2004.
- [44] A. M. Figueroa, R. Juárez-Ramírez, S. Inzunza, and R. Valenzuela, "Implementing adaptive interfaces: A user model for the development of usability in interactive systems," International Journal of Computer Systems Science and Engineering, vol. 29, no. 1, pp. 95-104, 2014.
- [45] P. Zhang, "Integrating Human-Computer Interaction Development into SDLC: A Methodology," Communications of the Association for Information Systems, Vol. 15 , Article 29, 2005.
- [46] J. Liu, C. K. Wong, K. K. Hui, "An Adaptive User Interface Based on Personalized Learning", Journal IEEE Intelligent Systems, 18(2), pp. 52-57, March 2003.
- [47] E. Zudilova-Seinsträ, "On the role of individual human abilities in the design of adaptive user interfaces for scientific problem solving environments," Knowledge and Information Systems, vol. 13, no. 2, pp. 243-270, 2007.
- [48] V. López-Jaquero and F. Montero, "A seamless development process of adaptive user interfaces explicitly based on usability properties," Lecture Notes in Computer Science, vol. 3425, pp: 289-291, 2005.
- [49] C. Özgen, "Interface Design: Personal Preference Analysis," Master thesis, Middle East Technical University, Ankara, Turkey, 2008.
- [50] M. Bernard, C. H. Liao, and M. Mills, "The effects of font type and size on the legibility and reading time of online text by older adults," Proceeding of the Extended Abstracts on Human Factors in Computing Systems, pp. 175-176, 2001.
- [51] V. Evers and D. Day, "The role of culture in interface acceptance," International Conference on Human-Computer Interaction, no. 1993, pp. 260-267, 1997.
- [52] M. Just and D. Aspinall, "Personal choice and challenge questions: a security and usability assessment," Proceedings of the 5th Symposium on Usable Privacy and Security, Article No. 8, pp. 1-11, 2009.